Six Major Data Breach Trends From 2017

January 8, 2018 | By Jason Kravitz (https://securityintelligence.com/author/jason-kravitz/) Co-authored by Michelle Alvarez (https://securityintelligence.com/author/michelle-alvarez/)

Thinkstock (http://www.thinkstockphotos.com/image/stock-photo-analyzing-data/629202004/popup?sq=trends/f=CPHX/p=4/s=DynamicRank)

It seems like the moment the security industry collectively comes to grips with the latest publicly disclosed data breach, another bigger and badder security incident surfaces to shake it up, prompting many enterprises to worry if the same could happen to them.

Fortunately, by tapping into the overarching themes and patterns of these recent breaches, organizations can unlock insights to help them avoid becoming part of the breach news cycle.

Six Data Breach Trends From 2017 to Monitor in the New Year

IBM X-Force identified six major trends from over 235 publicly disclosed breaches it tracked in 2017. Some are trends that we've been highlighting for years, such as phishing attacks (https://securityintelligence.com/frost-sullivan-report-highlights-rise-in-phishing-attacks/) and failure to patch. Others are newer, growing trends, such as hijacked thingbots, misconfigured cloud servers and cryptocurrency-targeted attacks.

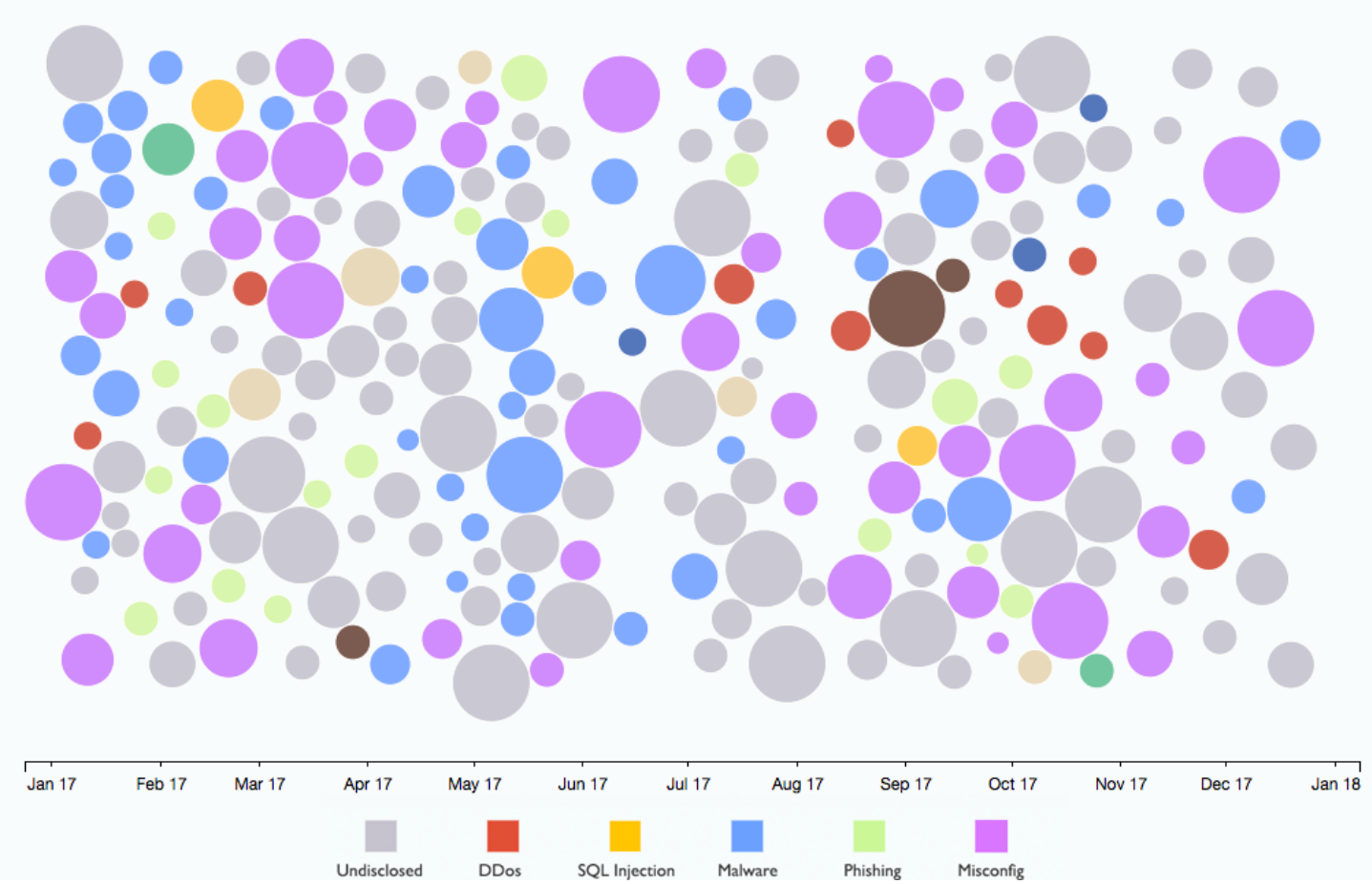

Figure 1: IBM X-Force tracked over 235 security incidents for 2017, comprising over 2.8 billion records (Source: IBM X-Force).

The security incidents described below represent only a few examples of each attack trend, which are listed in no particular order, and suggested mitigation tips, several of which fall under basic security hygiene (https://securityintelligence.com/back-to-basics-six-simple-strategies-to-strengthen-your-security-posture/). We all have an opportunity to learn from these incidents, and security professionals should pay close attention to notable trends, since they may indicate areas of possible concern in their own environments.

1. Bots of Things Attacking Other Things

What happens when millions of systems are exploited by a gaping remote vulnerability and then used as a botnet of zombie devices to launch distributed denial-of-service (DDoS) attacks or infect unsuspecting users with malware?

In August 2017, a consortium of six technology firms came together to take down WireX (https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/), a botnet comprised of tens of thousands of compromised Android devices that were being used to launch crippling DDoS attacks against targets in the hospitality industry. These vulnerable systems had been infected by more than 300 seemingly benign apps from the official Google Play store, including video players, file managers and ringtones. All these apps contained hidden code that could be activated for malicious use.

Threat such as the Mirai botnet (https://securityintelligence.com/the-internet-of-trouble-securing-vulnerable-iot-devices/), which turned hundreds of thousands of connected cameras and DVR devices into DDoS bots in November 2016 and struck again (http://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-attack-attempts-detected-south-america-north-african-countries/) toward the end of 2017, use the ability to commandeer a huge number of systems as a devastatingly effective attack tactic.

In September 2017, Armis Labs disclosed a Bluetooth vulnerability dubbed BlueBorne (https://www.armis.com/blueborne/) that could be exploited to silently take over any affected device within proximity of an attacker, potentially exposing billions of systems to compromise.

Related to this Article

WHITE PAPERS

IBM X-Force Research: Weaponizing the Internet of Things (https://securityintelligence.com/media/ibm-x-force-research-weaponizing-the-internet-of-things/)

(https://securityintelligence.com/media/ibm-x-force-research-weaponizing-the-internet-of-things/)

Malware that launches DDoS attacks or hijacks a device's CPU to mine cryptocurrencies (https://securityintelligence.com/network-attacks-containing-cryptocurrency-cpu-mining-tools-grow-sixfold/) can actually damage the hardware, since these devices were not made to sustain such high utilization. In December 2017, security researchers discovered that the prolonged execution of the CPU-intensive Loapi malware (https://securelist.com/jack-of-all-trades/83470/) caused the battery in their test Android phone to bulge out and deform the case.

All devices in your environment have the potential to become bots, including mobile devices. The time to begin identifying which IT assets could potentially be incorporated into botnet is not when a cybergang is actively using your devices to launch DDoS attacks. Organizations should consider managing the life cycle and inventory of assets through an IT asset management (ITAM) (https://www.ibm.com/security/endpoint-security/bigfix?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) program that also includes mobile device management (MDM) (https://www.ibm.com/security/maas360/mobile-device-management/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US).

The more these rising numbers of devices and endpoints use common libraries, platforms and operating systems, the more susceptible they are to the exploitation of a single vulnerability. In other words, aggregated risk goes through the roof in this scenario. The availability and growing ease of implementing scalable systems and architecture can lead to other problems as well.

2. Failure to Patch

Near close of business in Europe on Friday, May 12, 2017, a massive malware outbreak dubbed WannaCry (https://securityintelligence.com/unwrapping-the-mystery-did-a-big-slimy-internet-worm-make-hundreds-of-organizations-wannacry/) dumped ransomware onto Windows endpoints at hospitals, internet service providers (ISPs) and other critical targets. As IT professionals around the world scrambled to ensure that they were protected, it became evident that the worm was propagating via a Server Message Block (SMB) vulnerability, which had been patched by Microsoft (MS17-010) more than two months earlier. Similarly, NotPetya (https://securityintelligence.com/petya-werent-expecting-this-ransomware-takes-systems-hostage-across-the-globe/), another worm, used the same SMB vulnerability to propagate.

Widespread worms, such as Blaster and Sasser, were more common in the early 2000s, but seemed to have gone out of style as other types of attacks took form. Still, they illustrate the importance of keeping systems patched. Remediating critical unpatched vulnerabilities is key, so timely patch management is vital to organizations of any size.

While advanced zero-day attacks (https://securityintelligence.com/dont-just-put-out-the-zero-day-fire-get-rid-of-the-fuel/) can be a formidable threat, they are more often the stuff of fear and legend. In fact, according to the IBM X-Force vulnerability database, less than 1 percent of vulnerabilities in 2016 were considered zero-day vulnerabilities — that is, flaws exploited in the wild for which patches do not exist. Failure to patch existing critical vulnerabilities is most often the cause of havoc on a global scale, particularly when there is a huge number of vulnerable endpoints.

READ THE WHITE PAPER: REWRITING THE RULES OF PATCH MANAGEMENT (HTTPS://WWW-01.IBM.COM/MARKETING/IWM/DRE/SIGNUP?SOURCE=MRS-FORM-1941&S_PKG=OV37648&CE=ISM0484&CT=SWG&CMP=IBMSOCIAL&CM=H&CR=SECURITY&CCY=US)

3. Misconfigured Cloud Services

Cloud services enable companies to easily store millions of user data records for websites and apps. While vendors generally do a good job of securing these services, user error, misconfiguration and malicious insiders can publicly expose this data without providing any form of authentication.

Related to this Article

Leaking Cloud Databases and Servers Expose Over 1 Billion Records (https://securityintelligence.com/leaking-cloud-databases-and-servers-expose-over-1-billion-records/)

By Jason Kravitz (https://securityintelligence.com/author/jason-kravitz/)

(https://securityintelligence.com/leaking-cloud-databases-and-servers-expose-over-1-billion-records/)

This year alone, there have been numerous cases of misconfigured Amazon S3 buckets, Rsync backups, MongoDB databases and other similar services that exposed private, sensitive data. In July 2017, a third-party vendor that provided customer support services to a major telecommunications company exposed data (https://thehackernews.com/2017/07/over-14-million-verizon-customers-data.html) belonging to 14 million customers on a wide-open Amazon S3 cloud server. The data included custom personal identification numbers (PINs), which could be used to authenticate customer accounts.

As consumers, we download apps and services without much consideration for how they use or store our data. In one concerning breach (http://www.zdnet.com/article/popular-virtual-keyboard-leaks-31-million-user-data/) from November, security researchers uncovered a publicly accessible 577 GB MongoDB database (http://securityintelligence.com/get-serious-about-data-protection-to-secure-mongodb/) from an Israeli company that sells a keyboard app for mobile phones. The data not only contained usernames and emails addresses, but also location-based GPS information for users and transcripts of text that was typed into phones via the keyboard app.

The year closed with a massive leak affecting 123 million Americans after a misconfigured Amazon S3 bucket (https://www.upguard.com/breaches/cloud-leak-alteryx) allowed AWS Authenticated Users — that is, any user that has an Amazon AWS account — to download the stored data. This type of data is valuable to attackers, who can use it to target specific individuals and companies through spear phishing.

Cloud databases (https://securityintelligence.com/leaking-cloud-databases-and-servers-expose-over-1-billion-records/) leaked over 2 billion records in 2017. According to IBM X-Force, server misconfigurations made up 70 percent of the total number of reported leaked records this past year. It's important for organizations to conduct proper risk assessments of their cloud deployments. Security professionals should consider periodically engaging a professional penetration testing service (https://www.ibm.com/security/services/penetration-testing?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) to map vulnerabilities and inadvertent access issues.

Leaked data can have immense monetary value, especially when someone is willing to pay to keep it private. As we'll see in the next trend, attackers have homed in on new targets to exploit and extort to make money.

4. Cyberextortion of High-Value Data

In late April 2017, a popular video streaming service was informed that new episodes of one of its most popular shows had been stolen from a third party (https://arstechnica.com/information-technology/2017/05/orange-is-the-new-hacked-netflix-series-leaked-in-vendor-hack/) that provided postproduction services for the show. The threat actor also stole several other shows that had yet to be released and threatened to leak the files to the public if a ransom was not paid. A similar ransomware scheme (https://www.wired.com/story/hbo-hack-ransom-note/) emerged later in the year involving the theft of episodes from another popular show.

In addition, several plastic surgery clinics were breached this year, including one in Beverly Hills (http://abc7.com/news/socal-plastic-surgery-clinic-hit-with-massive-data-breach/2061144/) and one in London (https://www.thedailybeast.com/hackers-steal-photos-from-plastic-surgeon-to-the-stars-claim-they-include-royals), both of which catered to celebrity clients. Given the sensitive nature of photos and patient history, high-profile targets such as these are particularly vulnerable. Whether they're going after medical records, private dating preferences, intellectual property or hot television series, attackers are targeting high-value data in attempts to earn cash through good old-fashioned extortion.

Imagine that your data has been stolen from a third party with which you do business and is now being held for ransom. What is your game plan? Do you have outside counsel, crisis communications and incident response teams (https://www.ibm.com/security/services/xforce-incident-response-and-intelligence?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) on retainer to provide guidance? Do you

have a contact in law enforcement to disclose the breach to? How will you respond to the ransom demands? How will you address your customers and the media? An organization's response to a breach can potentially be just as damaging as the breach itself.

According to the "2017 Cost of Data Breach Study (https://www.ibm.com/security/data-breach?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US)" sponsored by IBM Security and conducted by Ponemon Institute, "an incident response (IR) team reduced the cost by as much as $19 per compromised record." Your incident response plan should be a dynamic document that is routinely reviewed, exercised and adjusted according to the results of a breach investigation.

5. Phishing Nets Big Targets

While stealing data and demanding ransoms is a lucrative tactic, some attackers have found that simply asking for money in a certain way can be quite effective.

Business email compromise (BEC) is a threat in which an attacker sends an email asking an employee to wire money or send confidential data, such as W-2 forms. These scams are often carried out by threat actors who impersonate C-suite executives and authority figures at precisely targeted companies.

Savvy attackers spoof these leaders' email accounts and mimic their writing styles to trick victims. Fraudsters netted more than $5 billion (https://www.ic3.gov/media/2017/170504.aspx) in stolen funds between 2013 and 2016 via BEC attacks. In 2017, DataBreaches.net (https://www.databreaches.net/victim-of-w-2-scams-2017-list/) tracked more than 200 companies that were tricked into sending employee W-2 forms to a malicious outsider. While phishing is often used in combination with other attacks, these BEC attacks illustrate how phishing alone can be highly lucrative for criminals.

Another BEC technique observed over the past year involved attackers registering domains that closely resembled those of vendors, such as construction firms, that were engaged in multimillion-dollar projects. For example, a Canadian university was tricked into sending nearly $12 million (https://globalnews.ca/news/3710654/macewan-university-loses-nearly-12m-in-phishing-scam/) to a cybergang posing as a trusted construction vendor.

These attacks are effective because defenses are often lowered when people mistake the attacker for a person inside their circle of trust. When a user sees an email coming from an authority figure or what looks like a trusted vendor, he or she might not think to double-check the sender's identity. This may be especially true in cases where there are fewer rungs on the corporate ladder, since it may not be unusual to receive an email from the CEO or CFO in a small or midsized company.

Phishing techniques such as BEC scams (https://securityintelligence.com/canadian-business-banking-customers-hit-with-targeted-phishing-account-takeover-attacks/) continue to plague users because they are highly successful. User education programs need to continuously change to keep up with the rapidly evolving threat landscape. For example, it is no longer sufficient to simply scan an email for misspellings or grammatical errors. The phishing lures are so convincing these days that even a seasoned security professional might have difficulty spotting a fraud. Users should alert the security team of suspicious emails and only open attachments they expect to receive.

Unfortunately, users tend to take a similar approach to installing software on their systems, putting their trust in vendors to deliver a secure product and legitimate updates.

6. Cryptocurrency Targets on the Rise

With the ever-rising valuation of bitcoin and other cryptocurrencies, these are quickly becoming a choice target for attackers. But stealing crypto coins is not new in 2017. In fact, some historic thefts over the years are even more significant today, given the exponential increase in price.

Consider the theft in 2016 of 119,756 BTC from a Hong Kong bitcoin exchange (https://techcrunch.com/2016/08/02/bitcoin-drops-20-after-70m-worth-of-bitcoin-was-stolen-from-bitfinex-exchange/), which, at the time, equated to $77 million. Today, that haul would be valued at over $1.5 billion. Similarly, a Slovenian Bitcoin exchange (https://thenextweb.com/hardfork/2017/12/07/bitcoin-exchange-nicehash-robbed-of-64-million-from-its-wallet/) was robbed in 2017 of 4,700 BTC, which, within a week of the theft, fluctuated in value by almost $20 million.

Initial coin offerings (ICO) are becoming popular vehicles to quickly fund an enterprising business through the sale of digital currency tokens while offering investors the potential for huge returns on their investment. ICOs have unsurprisingly become top targets for cybercriminals who, throughout 2017, devised creative ways to siphon funds and trick investors into wiring millions of dollars worth of cryptocurrency. Attackers hijacked the website of an Israeli company in the midst of its ICO and changed the wallet address (https://thehackernews.com/2017/07/ethereum-cryptocurrency-heist.html), which is similar to a long bank account number, to receive funds. In under three minutes, more than $7 million worth of Ethereum cryptocurrency was routed to the attackers.

Crafty criminals are targeting end users with some additional crypto-stealing malware techniques, such as intercepting and changing payment addresses in the clipboard to hijack payments and combing user files for crypto wallets and private keys, which could be used to steal funds.

Safe computing standards should be applied to the emerging world of digital money. Crypto veterans and new users alike should employ some basic practices to help protect their digital investments. At the very least, users should employ two-factor authentication (2FA) at crypto exchanges and websites. When trading or making payments, double- and triple-check the recipient address before sending to ensure that it wasn't changed or manipulated. For endpoint wallet attacks, consider using a hardware wallet, such as Trezor (https://wallet.trezor.io/) or Ledger (https://www.ledgerwallet.com/), to keep private keys on external devices that are protected by PINs.

Don't Wait to Address These Data Breach Trends

While many of these data breach trends have remained the same over the years, it's always helpful to take a step back and evaluate your own risk personally and professionally. Don't wait to implement these simple security best practices. Failure to do so could be disastrous, while a focus on boosting enterprisewide security hygiene just might keep your organization out of the latest batch of doom-and-gloom news headlines.

LISTEN TO THE PODCAST: 5 SECURITY PREDICTIONS THAT WILL TAKE HOLD IN 2018 (HTTPS://SOUNDCLOUD.COM/SECURITYINTELLIGENCE/NEW-YEAR-NEW-THREATS-5-SECURITY-PREDICTIONS-2018/)

Tags: Bitcoin (https://securityintelligence.com/tag/bitcoin/) | Bitcoin Mining (https://securityintelligence.com/tag/bitcoin-mining/) | Cloud Services Provider (https://securityintelligence.com/tag/cloud-services-provider/) | Cost of a Data Breach (https://securityintelligence.com/tag/cost-of-a-data-breach/) | Cryptocurrency (https://securityintelligence.com/tag/cryptocurrency/) | cryptocurrency miner (https://securityintelligence.com/tag/cryptocurrency-miner/) | Cybercrime Trends (https://securityintelligence.com/tag/cybercrime-trends/) | Data Breach (https://securityintelligence.com/tag/data-breach/) | Data Breaches (https://securityintelligence.com/tag/data-breaches/) | Internet of Things (IoT) (https://securityintelligence.com/tag/internet-of-things-iot/) | IoT Security (https://securityintelligence.com/tag/iot-security/) | Malware (https://securityintelligence.com/tag/malware/) | Patch (https://securityintelligence.com/tag/patch/) | Patch Management (https://securityintelligence.com/tag/patch-management/) | Phishing (https://securityintelligence.com/tag/phishing/) | Phishing Attacks (https://securityintelligence.com/tag/phishing-attacks/) | Ransomware (https://securityintelligence.com/tag/ransomware/) | Third-Party Vendors (https://securityintelligence.com/tag/third-party-vendors/) | Vulnerabilities (https://securityintelligence.com/tag/vulnerabilities/) | Vulnerability Management (https://securityintelligence.com/tag/vulnerability-management/)

RECOMMENDED ARTICLES

(https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/)

Threat Intelligence (https://securityintelligence.com/category/x-force/?subcat=threats)

IBM X-Force IRIS Uncovers Active Business Email Compromise Campaign Targeting Fortune 500 Companies (https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/)

By Alexandrea Berninger (https://securityintelligence.com/author/alexandrea-valentine/)

(https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/)

Threat Intelligence (https://securityintelligence.com/category/x-force/?subcat=threats)

TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of Wallets (https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/)

By Ophir Harpaz (https://securityintelligence.com/author/ophir-harpaz/)

(https://securityintelligence.com/necurs-spammers-go-all-in-to-find-a-valentines-day-victim/)

Malware (https://securityintelligence.com/category/x-force/?subcat=threats)

Necurs Spammers Go All In to Find a Valentine's Day Victim (https://securityintelligence.com/necurs-spammers-go-all-in-to-find-a-valentines-day-victim/)

By Limor Kessem (https://securityintelligence.com/author/limor-kessem/)

Jason Kravitz (https://securityintelligence.com/author/jason-kravitz/)

Techline Specialist, IBM Security

Jason Kravitz is an active editor and contributor to the IBM X-Force Trend and Risk Report, bringing a unique vision which melds diverse interests in security, photography, music, data visualization and graphic design, with two decades of experience as a software engineer.

SEE ALL POSTS →

FOLLOW

TRENDING ARTICLES

XMRig: Father Zeus of Cryptocurrency Mining Malware? (https://securityintelligence.com/xmrig-father-zeus-of-cryptocurrency-mining-malware/)

Read More (https://securityintelligence.com/xmrig-father-zeus-of-cryptocurrency-mining-malware/)

IBM X-Force IRIS Uncovers Active Business Email Compromise Campaign Targeting Fortune 500 Companies (https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/)

Read More (https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/)

TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of Wallets (https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/)

Read More (https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/)